2019-04-29

A Novel Transparent User Authentication Approach for Mobile Applications

Alotaibi, S

10.1080/19393555.2019.1609628
Information Security Journal: A Global Perspective
Taylor & Francis

A Novel Transparent User Authentication Approach for Mobile Applications

Saud Alotaibi[1], Steven Furnell[1, 2, 3] , and Nathan Clarke[1, 2]
[1]*Centre for Security, Communications and Network Research*
University of Plymouth
Plymouth, UK
[2]*Security Research Institute*
Edith Cowan University
Perth, Western Australia
[3] *Centre for Research in Information and Cyber Security*
Nelson Mandela University
Port Elizabeth, South Africa

{saud.alotaibi, steven.furnell, nathan.clarke}@plymouth.ac.uk

ABSTRACT

With the rapid growth of smartphones and tablets in our daily lives, securing the sensitive data stored upon them makes authentication of paramount importance. Current authentication approaches do not re-authenticate in order to re-validate the user's identity after accessing a mobile phone. Accordingly, there is a security benefit if authentication can be applied continually and transparently (i.e., without obstructing the user's activities) to authenticate legitimate users, which is maintained beyond point of entry. To this end, this paper suggests a novel transparent user authentication method for mobile applications by applying biometric authentication on each service within a single application in a secure and usable manner based on the risk level. A study involving data collected from 76 users over a one-month period using 12 mobile applications was undertaken to examine the proposed approach. The experimental results show that this approach achieved desirable outcomes for applying a transparent authentication system at an intra-process level, with an average of 6% intrusive authentication requests. Interestingly, when the participants were divided into three levels of usage (high,

medium and low), the average intrusive authentication request was 3% which indicates a clear enhancement and suggests that the system would add a further level of security without imposing significant inconvenience upon the user.

KEYWORDS: Transparent authentication, mobile applications, mobile security, usable security biometric authentication, smartphones, tablets.

1. Introduction

The use of mobile devices such as smartphones and tablets has grown steadily and has become an essential part of the daily lives for many people. Common examples of usage include activities such as sending emails, transferring money via mobile Internet banking, making calls, texting, surfing the Internet, viewing documents, storing medical, confidential and personal information, shopping online and playing games. Some of these active applications are considered sensitive and confidential, and the risks are high in the event of the loss of sensitive data as a result of privacy breaches (Tam et al., 2015; Patel et al., 2016). After authentication at the point of entry using techniques such as a personal identification number (PIN) or password, the user of the device can perform almost all tasks, of different risk levels, without having periodically to re-authenticate in order to re-validate the user's identity (Clarke et al. ,2009).

Furthermore, the current point-of-entry authentication mechanisms consider all applications on a mobile device to have the same level of importance and thus do not apply any further access control rules unless the applications themselves incorporate those (Clarke et al., 2009). As a result, Clarke et al. (2009) argue that different applications require different security provision. For instance, a bank account requires a different level of protection compared with a Short Message Service (SMS) message. Consequently, each application has a particular level of risk

which might be a feature for defining a suitable level of security (Ledermuller and Clarke, 2011).

It is also argued that, within a single mobile application, there are different processes operating on the same data but with differing levels of risk. For instance, the unauthorised disclosure or modification of mobile data has the potential to lead to a number of undesirable consequences for the user. Thus, there is no single level of risk associated with a given application and the risk level should, instead, change during use (Alotaibi et al., 2016). In this context, a novel mobile application data risk assessment model has been proposed to appreciate the risk involved within an application (intra-process security) (Alotaibi et al., 2016a). To this end, a transparent and continuous authentication mechanism provides a basis for convenient and secure re-authentication of the user and gathers user data in the background without requiring any dedicated activity (Clarke et al., 2009; Chuang et al., 2018).

This research suggests a novel transparent user authentication method for mobile applications by applying biometric authentication on the smartphone's application actions-level based on the risk level. For instance, WhatsApp application contains different level of action risks such as send a text message which is considered high risk whereas receiving an audio message is considered a medium risk and receive a free call (voice/ video) is considered low risk. In addition, mobile phones can be used to capture multiple biometric modalities such as facial recognition, voice recognition and fingerprint recognition by utilising microphones, camera, keypads and GPS without disturbing the honest mobile users. More specifically, the user biometrics are captured and collected in the background by regularly and periodically checking user behaviour in order to continuously monitor the protection of the smartphones. For instance, if the user uses the mobile phone for reading a message/email, watching a video, making or receiving a call or video conference, the mobile phone might be able to capture face samples. Furthermore, the system builds user biometric profile which is called user confidence

based on his biometric signals and when the user tries to access to a high-risk service such as transferring money form mobile banking application, the computed confidence has to be more than the threshold for this service, otherwise the system rejects and asking for PIN or username to be entered (intrusive authentication). In this study, after collecting a user's actions, the biometrics scenarios are applied.

Within the remainder of the paper, section two presents a review of current state-of-the-art literature on transparent and continuous authentication for mobile device security. Section three then presents a novel transparent user authentication mechanism for mobile applications, followed by the research methodology employed. A full experimental study is presented in section four to test and discuss the proposed approach. Finally, conclusions and future work are highlighted in section five.

2. Related work

In terms of usability and security, biometric authentication has been considered a reliable solution for authenticating users when compared with secret knowledge-based (password and PIN) and token-based (smart cards) approaches (Al Abdulwahid et al., 2016; Zhang et al., 2018). Biometrics are classified by their use of physiological biometrics, such as fingerprint scanning or face recognition, or behavioural biometrics, such as keystrokes or touch. Physiological biometrics are commonly considered useful mainly for one-off authentication (De Marsico et al., 2015; Meng et al., 2015) because they require considerable computing power and high-quality images, which are not easy to obtain (Meng et al., 2015). For instance, iris recognition needs the user to face the camera, takes more time for authentication and requires high-cost additional hardware (Meng et al., 2015). Moreover, there are still challenges for iris recognition, such as detection, segmentation, coding, and matching (De Marsico et al., 2015). Fingerprint recognition suffers in the presence of poor conditions, such as cuts and dirt

(De Marsico et al., 2013). As a result, iris and fingerprint scanning methods are considered intrusive (Clarke, 2011). In contrast, behavioural biometrics refer to something the user does, such as typing, gait, application usage, voice or signature, which are considered to be less sensitive to, for example, darkness or noise (Tanviruzzaman and Ahamed, 2014).

Clarke (2011) defines Transparent Authentication Systems (TAS) as follows: "Transparent authentication can be achieved by any authentication approach that is able to obtain the sample required for verification non-intrusively". In this context, TAS can be described in terms such as implicit, passive, non-intrusive, unobtrusive, unobservable, active, and silent. Google, for example, has plans to use a continuous and transparent authentication mechanism instead of user name and password (Hatin et al, 2017). Furthermore, Gartner estimates that behavioural biometrics will replace passwords by 2022 (Data Protection Centre, 2018).

In addition, behavioural biometrics are presented as a suitable method and are more commonly used for transparent and continuous authentication and for providing usability (Clarke, 2011; Hatin et al., 2017). In prior works, various behaviour-based authentications were presented to verify the rightful owner of a device, such as those based on touchscreen input behaviour, application usage, and patterns relating to keystrokes, calls and texts, voice, physical location and micro-movements (Khan and Hengartner, 2014), due to the ability of smartphones to gather a user's behavioural data without requiring deliberate actions from the user or additional hardware. For example, Apple has introduced a new patent for a "Fingerprint Sensor in an Electronic Device", in order to move the sensor from the home button to a new location below the touchscreen. This will allow fingerprints to be read from any point on the touchscreen surface (Yousefpor et al., 2014). Furthermore, although facial recognition suffers from certain problems, such as the difficulty of authentication in the dark and changes over time (Tresadern et al., 2013), it could be used in a transparent authentication system to collect a sample without effort from the user (Clarke, 2011). Therefore, biometrics can be employed to substantiate

whether the authenticated user is the true owner of the smartphone and maintain security. Apple has also introduced Face ID to provide secure authentication for the iPhone X (Apple, 2018; Juniper, 2018). Fingerprints will also be used for transparent authentication in the near future (Feng et al., 2012; Koundinya et al., 2014). In this context, TAS for mobile devices have been summarised and classified into the following (Alotaibi et al., 2015): keystroke, gate, touch, device sensor, and behavioural profiling.

A number of studies have investigated the feasibility of using behavioural biometrics to secure a mobile device, and several have proposed application usage aimed at providing transparent authentication. For instance, Hayashi et al. (2012) argue that device-centric continuous authentication cannot discriminate between data from different applications. More broadly, the authors argue that this method cannot make any assumptions in terms of the importance of the application currently being used. More specifically, not having a device-centric approach, and a lack of awareness of the task that the user is performing within an application, can lead to not delivering authentication control at the task level (Khan and Hengartner, 2014). This leads to higher authentication overheads. Hayashi et al. (2012) comment on the inefficiency of the all-or-nothing access model and suggest that a mobile user should be authenticated only when a sensitive application is begun, since most applications do not require explicit authentication. In the context of a sensitive application concept, the authors created paper prototypes (i.e., a theoretical method) for two alternative access mechanisms: group accounts and an activity lock. The group account would provide access to some of the functionality that is normally available only when the phone is unlocked. Thus, this group is for sharing non-sensitive information or applications. In comparison, an activity lock can be activated by the device owner before handing the device to another user to share specific screens in an application. Conversely, configuring a group account on a device enables the device owner to share a specific set of applications with other users.

In the same context, the work of Riva et al. (2012) is based on when the user should authenticate (as opposed to how) and for which application. The authentication decision depends on the levels of confidence and sensitivity for each application, which are stated by the user to protect sensitive applications from unauthorised use. The result of this prototype was a 42% reduction in requested explicit authentication, but was conducted with only nine users. A similar but more thorough study was conducted on positive (i.e., familiar events) and negative (i.e., unexpected changes of predictable places) habits. Among further studies in a similar context, Li et al. (2011) introduced a behaviour profiling approach to identify mobile device misuse by focusing on the mobile user's application usage; namely, general application usage, voice calls, and text messaging. The proposed approach achieved a total Equal Error Rate (EER) of 7.03%.

Efforts have also been made to investigate the feasibility of combining biometric modalities to authenticate a mobile user. Clarke et al. (2009) proposed a framework called Non-Intrusive Continuous Authentication (NICA) to provide secure, transparent and continuous authentication. NICA uses keystroke dynamics, facial recognition and voice patterns to inform the alert level while the user interacts with the mobile device. NICA is based on 'authentication confidence', which is mapped to each service in order to allow the user to access a service if the confidence level is higher than the alert level. In this work, the authors take into account the hypothesis that different services require varying levels of security and protection by understanding the risks associated with specific user actions and services, such as transferring money from an online banking application.

Crawford et al. (2013) introduced a transparent authentication framework utilising a combination of behavioural biometrics: keystroke dynamics and voice recognition based on device confidence level. In this research, each task on a device is assigned a particular device confidence level as the minimum threshold for access to the task, either explicitly by the owner or by default. As a result, private or sensitive information can be accessed only at the highest

device confidence level. This method is similar to online banking systems, in which the user needs to perform a task that might have side effects: the bank system requires a further authentication step for the user to be authorised (Crawford et al., 2013).

Similarly, Saevanee et al. (2012) examined the combination of three diverse biometric methods: keystroke dynamics, behavioural profiling and linguistic profiling. By using this multimodality, they achieved a total EER of 3.3% from 30 virtual users (this dataset was not real and was gathered from different datasets). To continue their work, Saevanee et al. (2014) presented a text-based authentication framework utilising those modalities and introduced a level of security by allowing the user to set different security levels for accessing different applications. The researchers claim that this approach would reduce the number of intrusive authentication requests for high-security applications by 91%. Likewise, Fridman et al. (2015) proposed a parallel binary decision-level fusion architecture for active authentication. This fusion is used for classifiers based on four biometric modalities: text analysis, application usage patterns, web browsing behaviour, and the physical location of the device by computing GPS (outdoors) or Wi-Fi (indoors) coordinates. To evaluate this framework, the authors collected a dataset from 200 users' Android mobile devices for 30 days. After one minute of the user using the device, the ERR was 5%, whereas after 30 minutes the EER was 1%. Despite the promising results of this work, battery consumption was the main limitation.

Unlike previous work, the current research suggests the need to move an access control system from the application level (inter-process) to within the application (intra-process) based on the risk for each user action as shown in Figure 1. To the best of the authors' knowledge, applying a transparent authentication system to each process within an application based on the risk level has not been investigated previously.

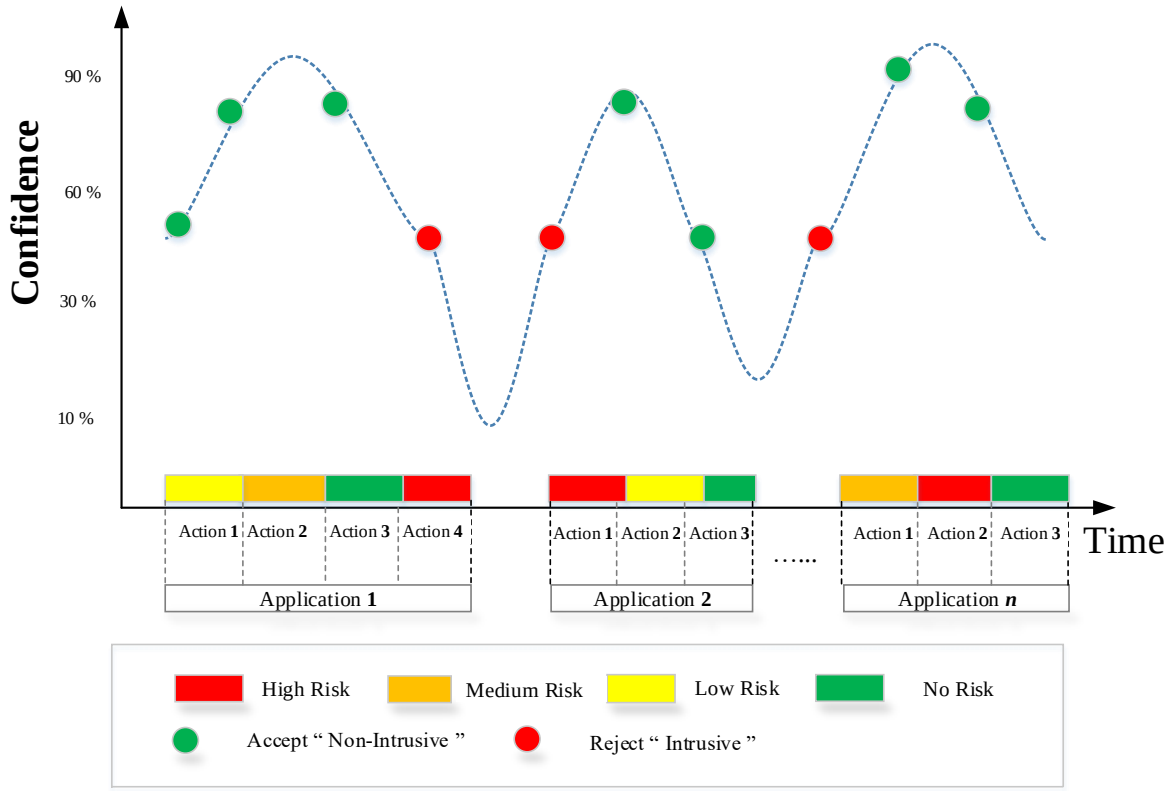

Figure 1. Identity Confidence and the actions risk level timeline

3. A Novel transparent user authentication approach for mobile applications

Having considered the contributions of prior work, the aim of this research is to propose an intelligent transparent authentication framework for intra-process security for mobile applications to fulfil security obligations and provide continuous protection by ensuring the validity of the current user. More specifically, this paper investigates the following research question:

> *Are transparent authentication systems applicable to intra-process resolution (within a given application) based on the risk level for each service in a secure, continuous, transparent manner by utilising a combination of device owner's biometrics based on the mobile user's usual interaction with an individual mobile device?*

3.1. A proposed framework

A framework based on Clarke and Furnell (2007) was used to address the above concept, as shown in Figure 2. The proposed framework consists of a number of key components, including a Data Collection Engine, a Biometric Profile Engine, and an Authentication Engine. These engines perform various tasks, such as collecting biometric data, generating user profiles, and verifying the user's identity, respectively. There are two main system components. The first is the Authentication Manager, which controls the three engines referred to previously, sets the confidence level, observes the current security level and makes authentication decisions if the user requests access to a service within the application (intra-process). The Authentication Manager achieves this by comparing the risk level value for this intra process, which is retrieved from the Risk Database, with the confidence level value, which is calculated by the Authentication Engine. If the process risk value exceeds the threshold (confidence level), the user will be allowed access. However, if the process risk value is less than the threshold, the user will be denied access to the service. The second main system component is the Intra-Process Determination System, which observes the user's action on a specific application. This value is passed to the Authentication Manager to compare with the risk value for the process (a predefined value). The risk value is based on this new component. The novel elements are the ability to determine and identify the current user action on the application (intra-process), which is the key task of the Intra-Process Determination System. The outputs from this component are the application name and the intra-process name within this application, both of which are sent to the Authentication Manager in order to decide the legitimacy of the user to accomplish the action or not.

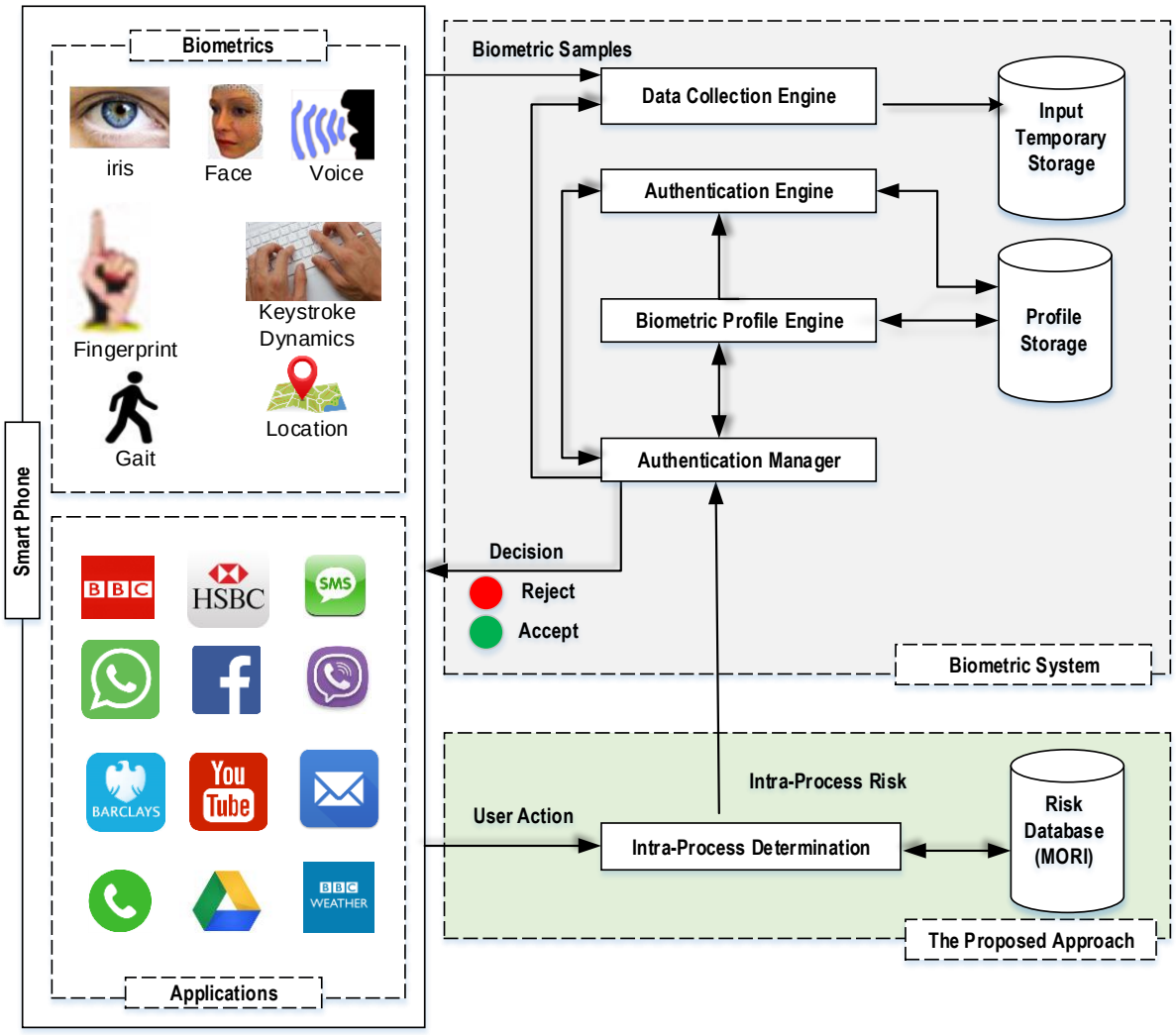

Figure 2. Framework for mobile application security (adapted from Clarke and Furnell, 2007)

To fully address the above research question, the following tasks were undertaken:

- Firstly: producing a novel mobile application data taxonomy (Alotaibi et al., 2016) and then introducing a novel mobile application data risk assessment model to understand the risk involved within an application (intra-process security). This investigation demonstrates that there is no single risk for using a given application, since the risk changes within the application from one process to another and determines the risk level for each process on a single application (Alotaibi et al., 2016a).
- Secondly: developing user action determination software in order to create a real dataset to utilise in the study experiments.

- Thirdly, conducting a series of experiments aimed at investigating the feasibility of the proposed system by testing the impact of the intra-process access on the overall transparent user authentication approach for mobile applications through a series of experimental analysis studies. These experiments were aimed at computing all intrusive user authentication requests by collecting log data from a total of 76 participants over a month of normal device usage.

3.2. Dataset

In order to investigate the feasibility of building a transparent and continuous biometric-based system, it is first necessary to collect samples of genuine user interactions with their mobile devices/apps based upon a substantive period of real-world use. As such, it was proposed to enlist participants and collect log data from them after one month of normal device usage. It should be noted that participation did not require the participants to do anything other than use their devices as normal. This experiment involved collecting the sort of data that are logged, such as a timestamp of the application used by the participant and the name of the user action (read, send, etc.). The experiment was carried out using the participants' Android mobile phones (start date: February 2017; end date: July 2017). For the purpose of this data collection, Python code was written utilising the Android Debug Bridge (ADB), which is a command line tool that allows communication with a connected Android device on a computer and was developed to extract log files from a backup file on the participants' devices after taking a backup .

In addition, some applications, such as Facebook, Online Mobile Banking, and Chrome, are fully encrypted, and there was no means of collecting user data without compromising users' privacy by asking the participants to root their device. For this reason, only 12 applications were collected, which were: Phone Call, SMS, Downloading, YouTube, WhatsApp, Browser,

Google Play, Email, Viber, Google Photo, Camera, and Yahoo mail. In which some users have used all of the listed applications while others used some of them. At the end of the collection process, data had been collected from 76 users and they were ready for the analysis phase. Each user's data were stored in an individual text file and each record contained the following fields: a date in two formats (human time and a timestamp e.g., 2016-06-28 20:22:30, 1467141750071), application name, action type, extra information, such as message/email length, and call duration.

3.3. Methodology

This experiment was conducted to explore the feasibility of building a transparent and continuous biometric-based system that would provide more secure and user-friendly authentication for mobile applications. The proposed approach was based upon assessing intra-process (within the application) user interactions and testing the impact of an intra-process approach on the overall transparent user authentication for mobile applications by including application access with other actions within the application for 76 participants. Before starting the data analysis, a risk model (MORI) (Alotaibi et al., 2016a) was used to calculate the risk level for each action within each application. Finally, each user's data were updated after applying the risk model and stored in an individual text file to calculate the possible biometrics and then confirm the identity of each user.

A wide range of biometrics were used in this research: facial, voice and iris recognition, keystrokes, behavioural and linguistic profiling, and fingerprint recognition, due to the ability of smartphones to capture multiple biometric modalities. Moreover, EERs published in prior studies in this domain were also used in this study. It was also considered that, if a user uses a mobile phone to read a message/email, watch a video, or make or receive a free call or video conference, the phone might be able to capture face samples. In this simulated scenario, therefore, a prior EER of 2% for facial recognition was selected (Tao and Veldhuis, 2010).

Likewise, EERs for finger samples of 3.74% (Raghavendra et al., 2013), keystroke samples of 2% (Zahid et al., 2009), voice recognition of 7.80% (Woo et al., 2006), iris samples of 0.12% (Chen et al., 2012), and linguistic profiling samples of 12.8% (Saevanee et al., 2015) were also selected. Moreover, if a user uses more than three application at a time, it might be possible to utilise a behavioural profiling biometric, so a prior EER of 7.03% was selected to assess this (Li et al., 2011).

In order to compute an identity confidence level based on the simulated biometric scenario, a weighted majority voting (WMV) formula (Al Abdulwahid, 2017) was utilised. In this approach, for each individual biometric technique, weights are assigned inversely proportionate to their EERs. More specifically, based on the WMV, a lower EER corresponds to a higher weighting than a high EER (Al Abdulwahid, 2017). Furthermore, a number of scripts were developed in order to extract the biometric information collected and identity confidence generated for each user to match the threshold which, in this research, was the risk level for each action.

NICA was selected to analyse the data and compute the identity confidence level (Clarke et al., 2009). The NICA framework is designed to be a mobile-based solution by utilising a combination of secret knowledge authentication and a number of biometric techniques in order to provide transparent and thus continuous authentication while the user interacts with the mobile device, despite an intrusive request at the beginning of the session (Clarke et al., 2009; Al Abdulwahid, 2017). In addition, the main aim of this framework is to observe the level of trust of the user in order to allow or restrict access to applications or services. Furthermore, based upon the biometric samples captured, the level of confidence fluctuates in a continuous manner (Clarke et al., 2009), which has an effect on permissions to access applications. More specifically, if no biometric samples are captured to cause the confidence level to exceed the threshold value, the device will be locked.

To provide effective security in a NICA system, two security mechanisms are considered imperative and define the core operation of the framework: Alert Level (AL) and Integrity Level (IL). These two levels are mapped to confidence levels to maintain security within the system, as well as its usability (Clarke et al., 2009; Al Abdulwahid, 2017). NICA has a function that is defined as a degradation function, to decrease the value of the Integrity Level (-0.5) periodically every 30 minutes for frequent users and 50 minutes for infrequent ones, as defined by NICA (2007), when the device is inactive.

During a specific time window, the AL process seeks valid samples. If there are no samples, the identity confidence level will be periodically reduced by a degradation function that is 10% of current confidence in order to protect the mobile device the mobile while it remains inactive. In the case of the mobile user requesting to perform a task, the IL is applied to check the legitimacy of the mobile user. If the identity confidence is greater than or equal to the specified risk action level, transparent access is allowed. Otherwise, an intrusive authentication request is required in order to proceed with the service.

In summary, each user file from the dataset was produced to generate different files. The first file was produced after applying the risk model (Alotaibi et al, 2016) and the second after generating possible biometric samples and then computing the identity confidence value. Finally, the two files were compared and matched at a specific time. If the confidence level is more than the threshold (action risk level), the user can access the service (non-intrusive authentication request); otherwise, the mobile device is locked (intrusive authentication request). This methodology was applied to each user file in order to compute the number of the intrusive authentication requests made during the intra-process (within the application) access to evaluate the average for the intrusive authentication requests for all 76 users. To do this, a number of scripts were generated and run with the participants' data for a combination of time windows: AL 2 min and IL 5 min; AL 5 min and IL 5 min; AL 5 min and IL 10 min;

AL 10 min and IL 10 min; AL 20 min and IL 10 min; and AL 20 min and IL 20 min. The reason for changing the time window each time was to provide further insight into whether this would affect the number of intrusive authentication requests for each user.

4. Experimental Results and Discussion

In this study, the main aim is to compute the number of intrusive authentication requests (i.e. entering PIN or username and password): the higher the percentage of intrusive requests becomes, the less usable the system. It should be noted that there is no need to calculate biometric accuracy such as false positive and false negative as the biometric was simulated.

With regard to the average user intrusive request distribution for intra-process access based on minimum, median, and maximum values over the differing time windows, the largest time window (AL=20/IL=20 min) achieved better results due to the majority of the average users' intrusive request distributions being less than 10% of the total average user intrusive request distribution. For instance, participant 35 achieved 13% intrusive authentication requests. In contrast, the shortest time window (AL=2/IL=5 min) achieved the worst result due to the majority of the average users' intrusive request distributions being about 20% of the total average user distribution. For instance, the average intrusive distributions for three of the participants (2, 29 and 46) were 37%, 36% and 38%, respectively. Interestingly, when the AL was the same value (e.g., AL=10/IL=10 min; and AL=10/IL=20 min), the average user intrusive request distribution was the same and the majority were less than 9%. Similarly, the case for the time windows AL=5/IL=5 min and AL=5/IL=10 min was the same, but the majority were near to 15%.

The experimental results for the percentages of intrusive authentication requests for six time windows for intra-process access were calculated and are summarised in Table 1, together with the numbers of intrusive users' requests. In Table 1, it seems clear that the average intrusive

requests decreased, ranging from 18% to 6%. In general, the larger the AL/IL time window, the fewer the authentication requests. This suggests there could be a high probability of capturing a number of biometric samples when a user interacts with the mobile device for long periods and does not recall a degradation function to reduce identity confidence when the device is inactive. However, this is not the case for short time intervals and does not, therefore, allow the mobile user to increase the identity confidence if the number of actions is low. In this context, the longest time window (AL=20/IL=20) attained the lowest average intrusive requests of 6%, which might act in the interests of usability but not security. The reasons there is no biometric samples while active degradation function at this short interval. More specifically, during the time window AL=2/IL=5 min, six participants (2, 12, 29, 46, 55 and 58) received more than 30% of the percentage of intrusive requests, possibly due to the total number of actions being very low compared with the total usage days and the number of actions per day. For instance, 27,576 actions were collected from participant 46 over 592 days, which represents about 46 actions per day. This low number of actions per day led to the highest number of intrusive requests of all the users (38%) and might affect the total average authentication requests (18%), as shown in Table 1.

Table 1. Average percentages of intrusive authentication requests

	Time window (min)					
	AL=2 IL=5	AL=5 IL=5	AL=5 IL=10	AL=10 IL=10	AL=10 IL=20	AL=20 IL=20
Average intrusive requests (%)	18	13	13	9	9	6
Total requests	3,006 k					
Intrusive requests ≤ 10% (# users)	16	29	27	45	46	67
10% < intrusive requests ≤ 15%	10	24	28	24	23	9
15% < intrusive requests ≤ 20%	21	9	14	6	6	0
Intrusive requests > 20%	29	14	7	1	1	0

One possible reason is that during the data collection stage, 47 actions were collected with the following distribution of risk types: high risk = 36%; medium risk = 47%; low risk = 13%; and no risk = 4%. As a result, the majority of these actions (83%) were considered to be high and medium risk. Figure 3 depicts the intrusive/non-intrusive request results with the types of risk for all the time windows, which, in turn, suggests that the identity confidence level should be higher to exceed the threshold for accessing the required service. The experimental results also show that the majority of intrusive requests came from high-risk actions. It seems to be the case that the majority of intrusive requests came from high-risk actions, only a few from medium-risk actions, and none from low-risk actions. For instance, for the AL=2/IL=5 min time window, 16% of the total average intrusive requests (18%) were triggered by high-risk actions and only 2% of the total average intrusive requests from medium-risk actions.

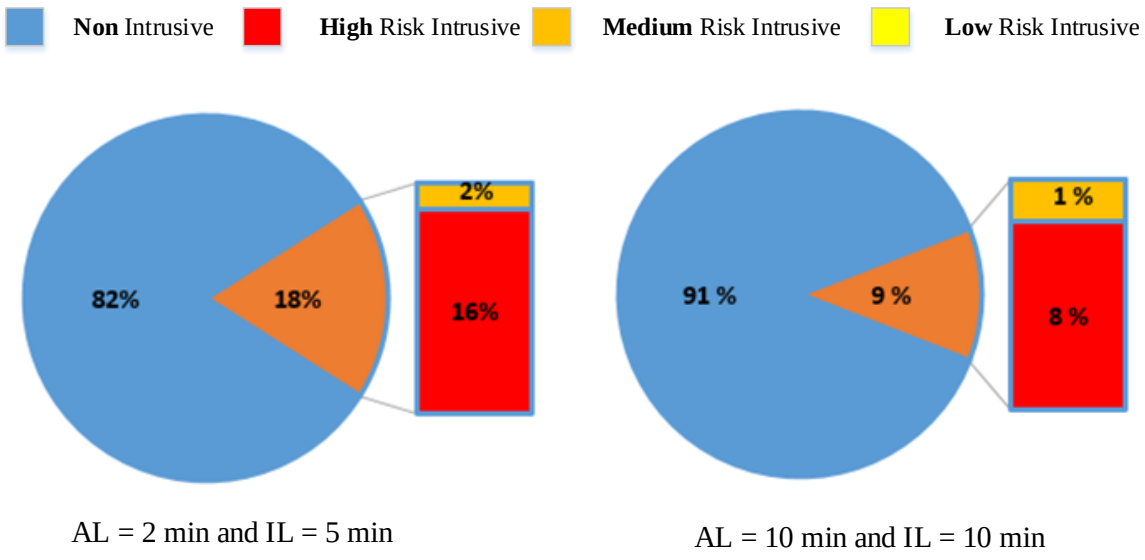

Figure 3. Intrusive/non-intrusive intra process results at AL=2/IL=5 min and AL=10/ IL=10 min

Further analysis was conducted to establish whether a particular grouping of time windows would perform better with a particular type of usage. To gain greater insight into how usage could affect the total average intrusive authentication requests for the entire dataset, the 76 users were categorised into three levels of group usage (high, medium and low) based on the

following average actions per hour (with the thresholds being set based upon values observed from the dataset):

> If (Actions per hour) > 5, then High Usage
> Elseif (Actions per hour) > 2, then Medium Usage
> Elseif Low Usage

As a result, there were 27 users with high usage, 24 users with medium usage, and 25 users showed low usage. After applying this methodology to the 76 participants, there was a clear need to investigate how low user usage would affect the total average intrusive authentication requests by recomputing the total average intrusive authentication requests for each usage group.

The following two figures (Figures 4 and 5) provide examples of the relation between the identity confidence levels and the intrusive authentication requests timeline for high user usage and low user usage, respectively. In Figure 4, the user confidence level continuously fluctuates based on the biometric samples captured, as does the risk level for the user action. Although there is a high fluctuation for this period, only one intrusive authentication request was triggered due to the biometric samples captured, thereby raising the identity confidence level for participant 57. In comparison, three intrusive authentications were requested during low user usage for participant 8. Furthermore, as seen in Figure 5, the user did not use the mobile from 18:11 PM until 18:32 PM and no biometric sample could be captured. For this reason, the confidence value was less than the threshold for accessing the required service and, therefore, the user was asked to enter a password or fingerprint for the authentication process. Similarly, no biometric samples could be captured between 19:01 AM and 19:23 PM and, as a result, identity verification decreased. However, the user's confidence level was very high after 19:32 PM, which suggests that the mobile user might have been able to take a high-risk action. This indicates that the more time between two consecutive actions, the greater the intrusive authentication requests.

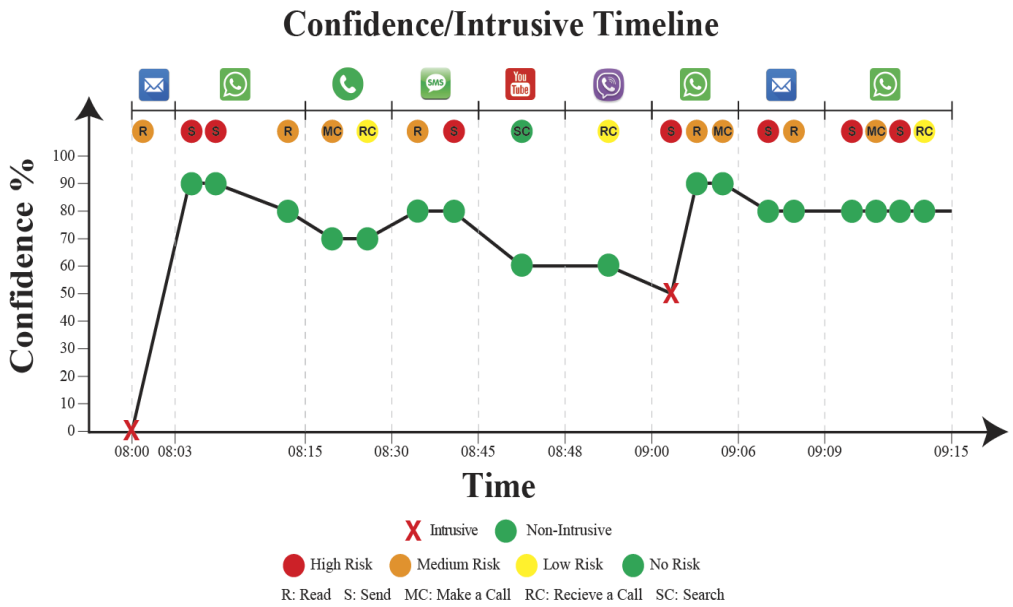

Figure 4. Confidence in relation to intrusive requests timeline for user 57 (high usage user)

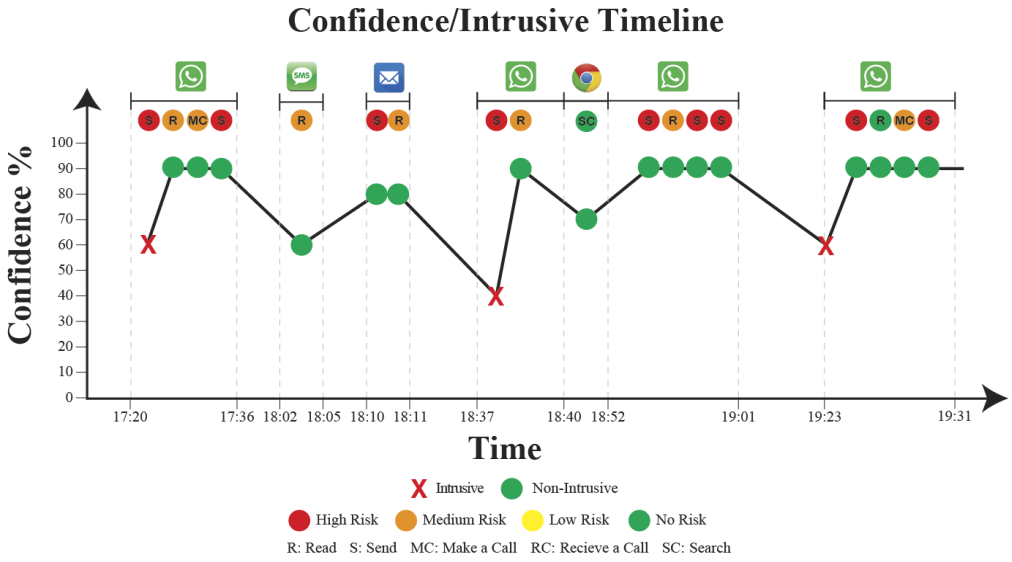

Figure 5. Confidence in relation to intrusive requests timeline for user 8 (low usage user)

The above results demonstrate that one of the time windows (AL=10/IL=10 min) achieved better results in the high usage group, as 95% of the users' intrusive authentication requests were under 8%. Similarly, in the medium usage group, 77% of the users' intrusive authentication requests were under 12%. However, half the users' intrusive authentication

requests were more than 14% for the low usage group. These experimental results suggest that AL=10/IL=10 min could be used for high usage and medium usage groups.

Based on the above experimental results for the percentage of intra-process intrusive authentication requests, the total requests for the six time windows were calculated and are summarised in Table 2. The information in Table 2 indicates that this approach achieved the best results after classifying participants into three usage groups (high, medium and low) and identifies suitable time windows for each group of users. Table 2 also shows that the larger the AL/IL time window, the fewer the intrusive authentication requests, perhaps due to the high probability of gathering biometric samples when the user interacts with the mobile device and not recalling the degradation function and reducing the identity confidence level when the device is inactive. In Table 2, the intrusive authentication requests achieved better results than those previously reported in the first experiment for all the different AL/IL timings. For instance, for the same time window (AL=5/IL=5 min), the percentage of average intrusive authentication requests for all users was 13% in table 1, but this was reduced to 7% for the high usage group in table 2. In contrast, the percentage of average intrusive requests increased to 21% after grouping the users in the medium usage group.

Furthermore, the number of participants whose percentage of intrusive authentication requests was less than 10% sharply increased and represented the majority of the participants for all the differing AL/IL timings. Interestingly, only one participant (58) achieved a percentage of 16% intrusive authentication requests in the AL=20/IL=20 min time window.

Table 2. Average percentages of intrusive authentication requests by usage

		Time window (min)					
		AL=2 IL=5	AL=5 IL=5	AL=5 IL=10	AL=10 IL=10	AL=10 IL=20	AL=20 IL=20
High usage	Average intrusive requests (%)	12	7	7	5	5	3
	Total requests	2,045 k					
	Intrusive ≤ 10% (# users)	6	21	21	27	27	27
	10% < intrusive ≤ 15%	14	6	6	0	0	0
	15% < intrusive ≤ 20%	5	0	0	0	0	0
	Intrusive > 20%	2	0	0	0	0	0
Medium usage	Average intrusive requests (%)	21	15	15	10	10	7
	Total requests	464,869					
	Intrusive ≤ 10% (# users)	1	2	2	13	13	24
	10% < intrusive ≤ 15%	2	14	14	11	11	0
	15% < intrusive ≤ 20%	10	7	7	0	0	0
	Intrusive > 20%	11	1	1	0	0	0
Low usage	Average intrusive requests (%)	22	16	16	13	13	9
	Total requests	496,096					
	Intrusive ≤ 10% (# users)	1	4	4	6	6	16
	10% < intrusive ≤ 15%	3	7	7	12	12	9
	15% < intrusive ≤ 20%	7	8	8	7	7	0
	Intrusive > 20%	14	6	6	0	0	0

It appears that the longest time window achieved a good result and reduced the number of intrusive authentication requests. For instance, the average intrusive authentication requests for AL=10/IL=10 min were fewer than for AL=5/IL=5 min by 2%. The change was clear for participants 28 and 48 by 5% and 2%, respectively. Interestingly, the experimental results for participant 71 for both time windows was the same for intrusive authentication requests at 3%. Furthermore, intrusive authentication requests changed very slightly (by 1%) for some of the participants: 3, 4, 11, 53, 60 and 64. However, there was a large difference between both time windows (AL=5/IL=5 min and AL=10/IL=10 min) for participants 15, 48, and 67, as the intrusive authentication requests reduced by 5% at the action level.

It also seems to be the case that the longest time window showed a good result for the medium usage group and the intrusive authentication requests reduced. Participants 2 and 12 achieved

a better result with regard to intrusive authentication requests (moving from 14% to 7% and from 12% to 6%, respectively). Similarly, for the low usage group, the longest time window also showed improved results (from 9% to 7% at the action level). Interestingly, intrusive authentication requests changed very slightly (by 1%) for some of the participants, such as 5, 22 and 72. In contrast, there was a significant difference at the action level for participants 29 and 46, whose intrusive authentication requests reduced by 3% (participant 29 moving from 14% to 11%). It appears that the majority of users achieved intrusive authentication requests of less than 10%.

In summary, Table 2 indicates that a large AL/IL time window leads to fewer intrusive authentication requests. A possible explanation for the largest time window outperforming the shortest time window could be that a high number of user interactions with the mobile phone leads to the collection of many more biometric samples, thereby raising the identity confidence level. Furthermore, this study highlights a clear effect of AL value on average intrusive authentication requests. Likewise, recalling the degradation function significantly affected the total confidence level, which automatically dropped. This seems logical, as there could be few biometric samples or the modality might be poor in the case of a short time window. A further point to be noted in these results is that the vast majority of intrusive requests came from high-risk actions and very few from medium-risk actions, whereas there was full transparency for low-risk actions. With regard to the system's robustness and users' convenience, a short time window is likely to lead to a large percentage of intrusive authentication requests, which could become a problem and disturb the mobile's legitimate user. However, short time windows would lower the security of the system, which might, in turn, allow imposters to access services.

5. Conclusions

This paper presented and evaluated a novel framework for transparent user authentication for mobile applications. An experiment was devised to explore the intra-process (within the application) access levels across different time windows. In summary, the experimental results demonstrate that this approach achieved results that would fulfil security obligations and a desirable level of results for applying a transparent intra-process authentication system. The shortest time window (AL=2/IL=5 min) produced an average of 18% intrusive authentication requests, whereas the largest time window (AL=20/IL=20 min) generated 6%.

Interestingly, when the participants were divided into three levels of usage, the average intrusive authentication requests were 12% and 3% for the shortest (AL=2/IL=5 min) and longest (AL=20/IL=20 min) time windows, respectively for the high usage group. To examine the results more closely, further investigation was undertaken in order to explore how low usage would affect the total percentage of users' intrusive authentication requests, by classifying the 76 participants into different types of users to gain greater insight to optimise the performance results and determine whether a particular grouping of time windows would perform better with a particular type of usage. Classifying the participants into three usage groups (high, medium and low) indicated notable improvement and achieved promising experimental results with regard to intrusive authentication requests compared with those previously reported in the first experiment for all differing AL/IL timings, from the shortest time window (AL=2/IL=5 min) to the longest (AL=20/IL=20 min). The results for the three usage groups underline the evidence for the effect of low user usage on the total average intrusive authentication requests for the selected time windows. This result suggests that there is a suitable time window for each usage group. It further suggests that there is a high probability of gathering biometric samples when the user interacts with their mobile device and the degradation function is not recalled to reduce the identity confidence level when the device is inactive for very short intervals.

Acknowledgement

This research was undertaken with the support of the government of the Kingdom of Saudi Arabia - Ministry of Interior.

References

Al Abdulwahid, A., Clarke, N., Stengel, I., Furnell, S., & Reich, C. (2016). Continuous and transparent multimodal authentication: reviewing the state of the art. Cluster Computing, 19(1), 455-474.

Al Abdulwahid, A., Federated Authentication using the Cloud (Cloud Aura). (2017). PhD thesis, Plymouth University.

Alotaibi, S., Furnell, S. & Clarke, N. (2015). Transparent authentication systems for mobile device security: A review. In the 10th International Conference for Internet Technology and Secured Transactions (ICITST) (pp. 406-413). IEEE.

Alotaibi, S., Furnell, S., & Clarke, N. (2016). A novel Taxonomy for mobile applications data. Int. J. Cyber-Security Digit. Forensics, 5 (3), 115-121.

Alotaibi, S., Furnell, S., & Clarke, N. (2016a). MORI: An Innovative Mobile Applications Data Risk Assessment Model. In Journal of Internet Technology and Secured Transactions (JITST), Volume 5, Issues 3/4.

Clarke, N., Furnell, S., Lines, B., & Reynolds, P. (2003). Keystroke dynamics on a mobile handset: A feasibility study .Information Management and Computer Security, vol. 11, no. 4, pp.161-166.

Clarke, N., Karatzouni, S., & Furnell, S. (2009). Flexible and transparent user authentication for mobile devices, IFIP Advances in Information and Communication Technology, 297/2009, pp.1-12.

Clarke, N. (2011).Transparent user authentication: biometrics, RFID and behavioural profiling, Springer Science & Business Media.

Chen, R., Lin, X., & Ding, T. (2012). Liveness detection for iris recognition using multispectral images. Pattern Recognition Letters, 33 (12), 1513–1519.

Chuang, Y. H., Lo, N. W., Yang, C. Y., & Tang, S. W. (2018). A Lightweight Continuous Authentication Protocol for the Internet of Things. Sensors, 18(4), 1104.

Crawford, H., Renaud, K., & Storer, T. (2013). A framework for continuous, transparent mobile device authentication. Computers & Security, 39, 127-136.

Data protection centre. (2018) Retrieved from http://dataprotectioncenter.com/access-control-2/behavioral-biometrics-will-replace-passwords-by-2022-gartner/

De Marsico, M., Galdi, C., Nappi, M., & Riccio, D. (2014). FIRME: Face and Iris Recognition for Mobile Engagement, Image and Vision Computing, vol. 32, no. 12, pp.1161-1172.

De Marsico, M., Nappi, M., Riccio, D., & Wechsler, H. (2015). Mobile Iris Challenge Evaluation (MICHE)-I, biometric iris dataset and protocols." In Pattern Recognition Letters. Elsevier Ltd., pp.17–23.

Dinca, L. M., & Hancke, G. P. (2017). The fall of one, the rise of many: a survey on multi-biometric fusion methods. IEEE Access, 5, 6247-6289.

Feng, T., Liu, Z., Kwon, K., Shi, W., Carbunar, B., Jiang Y., & Nguyen, N., (2012). Continuous mobile authentication using touchscreen gestures, in IEEE HST, pp.451–456.

Fridman, L., Weber, S., Greenstadt, R. & Kam, M. (2015). Active authentication on mobile devices via stylometry, application usage, web browsing, and GPS Location." In arXiv preprint arXiv, pp.1–10.

Hatin, J., Cherrier, E., Schwartzmann, J., & Rosenberger, C. (2017). Privacy preserving transparent mobile authentication. In International Conference on Information Systems Security and Privacy (ICISSP). pp. 354-361.

Hayashi, E. Riva, O. Strauss, K., Brush, A., & Schechter, S. (2012). Goldilocks and the two mobile devices: going beyond all-or-nothing access to a device's applications. In Proceedings of the Eighth Symposium on Usable Privacy and Security, ACM.

Khan, H. & Hengartner, U., (2014). Towards application-centric implicit authentication on smartphones. In Proceedings of the 15th Workshop on Mobile Computing Systems and Applications, p.1-6, February 26-27, 2014, Santa Barbara, California.

Koundinya, P., Theril, S., Feng, T., Prakash, V., Bao, J., & Shi, W. (2014). Multi-resolution touch panel with built-in fingerprint sensing support. In: Design, Automation & Test in Europe Conference & Exhibition (DATE), pp. 1–6. IEEE Conference Publications, New Jersey.

Ledermuller, T., & Clarke, N. (2011). Risk assessment for mobile devices. In Trust, Privacy and Security in Digital Business (pp. 210-221). Springer Berlin Heidelberg.

Li, F., Clarke, N., Papadaki, M., & Dowland, P. (2011). Misuse detection for mobile devices using behaviour profiling. IJCWT, vol. 1, no. 1, pp.41– 53.

Meng, W., Wong, D., Furnell, S., & Zhou, J. (2015). Surveying the development of biometric user authentication on mobile phones. IEEE Communications Surveys & Tutorials (Volume: 17, Issue: 3). pp. 1268 – 1293.

Meraoumia, A., Kadri, F., Bendjenna, H., Chitroub, S., & Bouridane, A. (2017). Improving biometric identification performance using PCANet deep learning and multispectral palm print. In Biometric Security and Privacy (pp. 51-69). Springer.

Patel, V. M., Chellappa, R., Chandra, D., & Barbello, B. (2016). Continuous user authentication on mobile devices: Recent progress and remaining challenges. IEEE Signal Processing Magazine, 33(4), pp. 49-61.

Raghavendra, R., Busch, C., & Yang, B. (2013). Scaling-robust fingerprint verification with smartphone camera in real-life scenarios. In Biometrics: Theory, Applications and Systems (BTAS). IEEE Sixth International Conference on (pp. 1-8).

Riva, O., Qin, C., Strauss, K, K., & Lymberopoulos, D. (2012). Progressive authentication: Deciding when to authenticate on mobile phones. In Proceedings of the 21st USENIX Conference on Security Symposium, ser. Security'12. Berkeley, CA, USA: USENIX Association.

Saevanee, H., Clarke, N., & Furnell, S. (2012). Multi-modal behavioural biometric authentication for mobile devices. In Proceedings of the Information Security and Privacy Research, IFIP Advances in Information and Communication Technology - IFIP AICT. Springer Boston. pp. 465-474.

Saevanee, H., Clarke, N., Furnell, S., & Biscione, V. (2014). Text-based active authentication for mobile devices. In ICT Systems Security and Privacy Protection. Berlin Heidelberg: Springer, pp.99-112.

Tam, K., Khan, S., Fattori, A. & Cavallaro, L. (2015). CopperDroid: Automatic Reconstruction of Android Malware Behaviors. In Proceedings of the 22nd Annual Network and Distributed System Security Symposium (NDSS'15), pp.1-15.

Tanviruzzaman, M., & Ahmed, S. (2014). Your phone knows you: almost transparent authentication for smartphones. In IEEE 38th Annual Computer Software and Applications Conference, pp. 374–383.

Tao, Q., & Veldhuis, R. (2010). Biometric authentication system on mobile personal devices. IEEE Transactions on Instrumentation and Measurement, 59(4), 763-773.

Tresadern ,P. , Cootes ,T., Poh ,N., Matejka ,P., Hadid ,A., Levy ,C., & Marcel ,S. (2013). Mobile Biometrics (MoBio): joint face and voice verification for a mobile platform". In IEEE pervasive computing, pp.79–87.

Woo, R. H., Park, A., & Hazen, T. J. (2006). The MIT Mobile Device Speaker Verification Corpus: Data Collection and Preliminary Experiments. In IEEE Odyssey 2006: The Speaker and Language Recognition Workshop. (Vol. 0, pp. 1–6).

Yousefpor, M., Bussat, J., Lyon, B., Gozzini, G., Hotelling, S., & Setlak, D. (2014). Fingerprint sensor in an electronic device", U.S. Patent Application 14/451,076.

Zahid, S., Shahzad, M., Khayam, A., & Farooq, M. (2009). Keystroke-based user identification on smart phones. In Recent Advances in Intrusion Detection. Berlin Heidelberg: Springer, pp.224-243.

Zhang, J., Tan, X., Wang, X., Yan, A., & Qin, Z. (2018). T2FA: Transparent Two-Factor Authentication. In IEEE Access, 6, pp.32677-32686. DOI: 10.1109/ACCESS.2018.2844548